KASPERSKY PRIVATE SECURITY NETWORK

Real-time, cloud-assisted cybersecurity for privacy-and-compliance-restricted networks.

It takes up to four hours for standard security solutions to detect, record and block the 325,000+ new malicious programs Kaspersky Lab researchers detect every day. Kaspersky Private Security Network takes about 40 seconds – without a single piece of data leaving your local network.

Kaspersky Private Security Network can be installed within the organization's own data center; in-house IT specialists retain complete control over it. You keep all the benefits of cloud-assisted security without compromising on privacy.

SUITABLE FOR:

- Enterprise customers with strict data control requirements
- Government agencies and organizations
- Telecommunications companies
- Service providers

KEY BENEFITS

- Identify the source of malware and prevent its spread
- Minimize the damage caused by cybersecurity incidents
- Reduce false positives
- Identify and differentiate between targeted attacks and more general threats
- Assess incident investigation and remediation requirements

Highlights

ALL THE BENEFITS OF CLOUD-ASSISTED SECURITY – WITHOUT THE NEED TO SHARE INFORMATION OUTSIDE THE LOCAL NETWORK:

- Unique threat intelligence on the latest, most sophisticated attacks, delivered within the controlled, local network
- Comply with strict regulatory, security and privacy standards
- Adapt for critical network isolation – including 'air gap' requirements
- Real-time protection from advanced threats – without the need to transfer data outside the organization
- Flexible deployment and piloting options
- Ready for MSSP/ISP installation.

Kaspersky Private Security Network is easy to test and deploy: just 1-2 standard servers are all you need to start benefitting from real-time threat intelligence.

Features

GLOBAL THREAT INTELLIGENCE FOR PRIVATE NETWORKS
Receive the latest threat intelligence in real time. Enhance protection, detection and reaction times while reducing false positives using the very best reputational analysis. File hashes, regular expressions for URLs and malware behavior patterns are centrally stored and categorized for rapid availability.

FILE REPUTATION SERVICE
Kaspersky Private Security Network service provides information about files by hash sum. Receive details including:

- File verdict: Good/Bad/Unknown
- File category: Browsers/Developer tools/Entertainment/Internet/Multimedia/Networking/OS & Utilities etc
- File digital signature
- File popularity

Verdicts and categories are compared against Kaspersky Lab's constantly updated dynamic whitelist, which contains over a billion files, enabling accurate blocking of malicious or unwanted files, with low false positive rates.

URL REPUTATION SERVICE

Kaspersky Private Security Network's URL reputation service provides information on 'safe' as well as malicious online resources (e.g. sites containing malicious links, malware or phishing):

- Verdict: Good/Bad/Unknown
- Category: Phishing/Malware/Web mail/Online Shopping/Social Networking/Job Sites/Adult Content/Gaming/Gambling etc

PATTERN-BASED SIMILARITY

Detect and identify any program or application's behavior using Kaspersky Lab's products, building a heuristic pattern capable of identifying it, or any malicious changes to it.

COMPLIANCE WITH CRITICAL NETWORK ISOLATION SECURITY STANDARDS

Kaspersky Private Security Network is installed entirely within the organizational perimeter –and operates within those limits only. This enables organizations with strict data privacy obligations – such as financial services or government agencies – to benefit from cloud-assisted security without compromising on privacy.

MSA ENTERPRISE INCLUDED

Maintenance and Support Agreement (MSA) is included with every installation: including highest priority 24x7x365 services, 30 minute response time[1] and a dedicated Kaspersky Technical Account Manager.

SYSTEM REQUIREMENTS

Kaspersky Private Security Network is a software-based solution for installation on physical or virtual servers.

Server configuration:
2 units (4 in high-availability set-ups):

- File + URL reputation: 1 unit
- Other KPSN Services servers: 1 unit

Server unit configuration:

- 2 CPU – 3.3GHz, 4 cores
- 256Gb RAM
- 300Gb HDD

Network requirements:
Two network interfaces of 1Gbps each.

Software requirements:

- Debian OS v8.2
- Google Chrome™, Mozilla™ Firefox™ or Opera browser
- Java plug-in version 7 or higher.

[1] Time between incident logging and provision of qualified response for 'Severity 1' incidents